Poczta

Poczta oparta na systemie Debian z Postfix, Dovecot, MySQL i Roundcube. Protokoły SMTP, IMAP, POP3 - szyfrowane. Webmail wraz z filtrowaniem wiadomości, regułami oraz autoresponderem.

Wstęp

Wszędzie gdzie pojawia się fraza domain.ltd należy zastąpić swoją domeną.

Instalujemy czystego Debiana 10 (Serwer SSH i Podstawowe narzędzia systemowe).

Jeśli system postawiliśmy na maszynie wirtualnej to proszę dodać taki oto wpis do pliku /etc/sysctl.conf:

```
net.ipv4.tcp_window_scaling = 0
```

Oraz przeładować ustawienia kernela:

```
sysctl -p
```

Uaktualnienie systemu:

```
apt update
apt upgrade
```

Instalujemy pakiety opcjonalnie (ułatwią pracę):

```
apt install aptitude mc unzip mailutils net-tools ntp
```

Plik /etc/hosts powinien mieć wpis z naszą domeną:

```
127.0.0.1       localhost
127.0.0.1       domain
127.0.0.1       domain.ltd

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Certyfikat SSL

Ważnym elementem jest szyfrowanie komunikacji między serwerem, a klientem - do tego jest wymagany certyfikat SSL. Certyfikat możemy uzyskać na trzy sposoby:

- wygenerować sobie samemu - wadą takiego rozwiązania jest to, że przeglądarka internetowa oraz klient poczty będzie ostrzegał, że certyfikat nie jest podpisany przez zaufaną instytucję -

nie polecam
- uzyskanie darmowego certyfikatu Let's Encrypt - wadą takiego rozwiązania jest to, że trzeba go odnawiać raz na trzy miesiące - da radę to zautomatyzować, jeśli nie możecie sobie poradzić z certbotem to tu możecie wygenerować sobie za free: https://www.sslforfree.com
- kupienie certyfikatu

My dla tutejszego przykładu wygenerujemy sobie certyfikat SSL - natomiast wam zalecam uzyskanie certyfikatu Let's Encrypt lub kupno.

```
cd /etc/ssl/private/
openssl req -new -x509 -nodes -newkey rsa:4096 -keyout ssl.key -out ssl.crt
-days 3600
chmod 400 ssl.key
chmod 444 ssl.crt
```

Instalacja niezbędnych pakietów

Podczas instalacji zostaniemy zapytani w sprawie konfiguracji Posfixa - wybieramy: brak konfiguracji.

```
apt install postfix postfix-mysql postfix-pcre postgrey dovecot-core
dovecot-imapd dovecot-pop3d dovecot-lmtpd dovecot-mysql dovecot-sieve
dovecot-managesieved mariadb-server mariadb-client
```

MySQL

Ustawiamy hasło dla roota, usuwamy zdalny dostęp dla roota, usuwamy użytkownika anonimowego oraz testową bazę danych:

```
root@mars:/etc/ssl/private# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n]
New password:
Re-enter new password:
Password updated successfully!
```

```
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n]
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n]
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n]
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Dodajemy bazę i ustawiamy uprawnienia:

```
root@mars:/etc/ssl/private# mysqladmin create postfix
root@mars:/etc/ssl/private# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 59
Server version: 10.3.25-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.

MariaDB [(none)]> GRANT SELECT ON postfix.* TO 'postfix'@'127.0.0.1'
IDENTIFIED BY 'tajnehaslo';
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> \q
Bye
```

Zapisujemy schemat bazy danych do pliku /root/postfix.sql:

```
CREATE TABLE virtual_aliases (
  id int(11) NOT NULL AUTO_INCREMENT,
  source varchar(128) NOT NULL,
  destination varchar(128) NOT NULL,
  PRIMARY KEY (id)
);

CREATE TABLE virtual_domains (
  id int(11) NOT NULL AUTO_INCREMENT,
  name varchar(64) NOT NULL,
  PRIMARY KEY (id)
);

CREATE TABLE virtual_users (
  id int(11) NOT NULL AUTO_INCREMENT,
  email varchar(128) NOT NULL,
  password varchar(128) NOT NULL,
  quota int(11) NOT NULL DEFAULT '1024' COMMENT 'Quota in megabytes',
  active tinyint(1) NOT NULL DEFAULT '1',
  PRIMARY KEY (id)
);

CREATE TABLE virtual_black_white_list (
  id int(11) NOT NULL AUTO_INCREMENT,
  source varchar(32) NOT NULL UNIQUE COMMENT 'Domain or IP address',
  access enum('OK','REJECT') NOT NULL COMMENT 'OK or REJECT',
  reason varchar(128) NOT NULL DEFAULT '',
  `type` enum('IP','EMAIL') NOT NULL,
  PRIMARY KEY (id)
);
```

Tworzymy tabele na bazie danych:

```
mysql postfix < /root/postfix.sql
```

Dodanie obsługiwanej domeny:

```
mysql -e "INSERT INTO virtual_domains (name) VALUES ('domain.ltd');" postfix
```

Dodanie konta email (domyślnie jest aktywne oraz ma pojemność 1GB):

```
mysql -e "INSERT INTO virtual_users (email, password) VALUES
('user@domain.ltd', ENCRYPT('haslo'));" postfix
```

Dodanie aliasu:

```
mysql -e "INSERT INTO virtual_aliases (source, destination) VALUES
('alias@domain.ltd', 'user@domain.ltd');" postfix
```

Blokada wcześniej założonej skrzynki:

```
mysql -e "UPDATE virtual_users SET active = 0 WHERE email =
'user@domain.ltd';" postfix
```

Odblokowanie skrzynki:

```
mysql -e "UPDATE virtual_users SET active = 1 WHERE email =
'user@domain.ltd';" postfix
```

Zmiana pojemności skrzynki na 2GB:

```
mysql -e "UPDATE virtual_users SET quota = 2048 WHERE email =
'user@domain.ltd';" postfix
```

Zmiana hasła dla skrzynki:

```
mysql -e "UPDATE virtual_users SET password = ENCRYPT('nowehaslo' WHERE
email = 'user@domain.ltd';" postfix
```

Dodanie do białej listy domeny:

```
INSERT INTO virtual_black_white_list (source, access, type) VALUES ('wp.pl',
'OK', 'EMAIL');
```

Dodanie do czarnej listy domeny:

```
INSERT INTO virtual_black_white_list (source, access, reason, type) VALUES
('spamers.ltd', 'REJECT', 'Your domain is in black list.', 'EMAIL');
```

Dodanie adresu IP do białej listy:

```
INSERT INTO virtual_black_white_list (source, access, type) VALUES
('1.2.3.4', 'OK', 'IP');
```

Dodanie adresu IP do czarnej listy:

```
INSERT INTO virtual_black_white_list (source, access, reason, type) VALUES
('2.3.4.5', 'REJECT', 'Your IP addressis in black list.', 'IP');
```

Domeny do białej/czarnej listy możemy definiować w następujący sposób:

- user@domain - adres email
- domain.ltd - cała domena
- .domain.tld - wszystkie subdomeny w danej domenie
- user@ - użytkownik we wszystkich domenach

Adresy IP definiujemy wg schematy CIDR. Dokumentacja: http://www.postfix.org/access.5.html

Możemy zarządzać bazą danych aplikacją napisaną pod w/w strukturę tabel:
https://gitlab.com/kmroczkowski/mailcp

Użytkownik skrzynek pocztowych

Katalogi skrzynek będą przechowywane z uprawnieniami użytkownika do obsługi skrzynek pocztowych, w naszym przypadku to będzie użytkownik vmail:

```
/sbin/groupadd -g 5000 vmail
/sbin/useradd -g vmail -u 5000 vmail -d /var/mail -s /bin/false
chown -R vmail:vmail /var/mail
chmod 750 /var/mail
mkdir /var/mail/vhosts
chown vmail:dovecot /var/mail/vhosts
chmod g+w /var/mail/vhosts
```

Postfix

Jeśli mamy swoją konfigurację już na serwerze to robimy backup plików postfixa:

```
cp /etc/postfix/main.cf /etc/postfix/main.cf.bak
cp /etc/postfix/master.cf /etc/postfix/master.cf.bak
/etc/init.d/postfix stop
```

Linki symboliczne do logów (opcjonalne):

```
ln -s /var/log /etc/postfix/logs
ln -s /var/mail/vhosts /etc/postfix/vhosts
```

W pliku /etc/mailname wpisujemy naszą domenę, którą będzie przedstawiał się Postfix:

```
domain.ltd
```

Konfiguracja w pliku /etc/postfix/main.cf (należy wyszukać frazę domain.ltd i zastąpić swoją domeną):

```
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
```

```
biff = no

append_dot_mydomain = no
readme_directory = no

compatibility_level = 2

# TLS parameters
smtpd_tls_auth_only = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_tls_security_options = noanonymous
smtpd_tls_cert_file=/etc/ssl/private/ssl.crt
smtpd_tls_key_file=/etc/ssl/private/ssl.key
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
smtp_tls_security_level = may
smtpd_tls_security_level = may
smtpd_tls_mandatory_ciphers = high
tls_high_cipherlist=EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA38
4:EECDH+aRSA+SHA256:EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!
aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-
SHA:AES256-SHA:CAMELLIA128-SHA:AES128-SHA
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3
smtpd_tls_loglevel = 1
smtp_tls_loglevel = 1

smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes

myhostname = domain.ltd
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = $myhostname
mydomain = $myhostname
mydestination = localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
#zalaczniki 100MB
message_size_limit = 102400000
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all

smtpd_sender_login_maps = mysql:/etc/postfix/mysql-virtual-sender-login-
maps.cf

smtpd_recipient_restrictions = check_policy_service inet:127.0.0.1:12340,
```

```
                                permit_sasl_authenticated,
                                permit_mynetworks,
                                reject_unauth_destination,
                                check_client_access
mysql:/etc/postfix/mysql-virtual-access-ip.cf,
                                check_sender_access
mysql:/etc/postfix/mysql-virtual-access-email.cf,
                                reject_non_fqdn_hostname,
                                reject_non_fqdn_sender,
                                reject_non_fqdn_recipient,
                                reject_unauth_pipelining,
                                reject_invalid_hostname,
                                reject_rbl_client sbl.spamhaus.org,
                                reject_rbl_client bl.spamcop.net,
                                reject_rbl_client cbl.abuseat.org,
#                               reject_rbl_client dnsbl.sorbs.net, #ostatnio
maile z gmail wpadały do tej spamlisty - tymczasowo wyłączyłem u siebie
                                reject_rbl_client zen.spamhaus.org,
                                check_policy_service inet:127.0.0.1:10023


smtpd_helo_restrictions =
        permit_mynetworks,
        permit_sasl_authenticated,
        reject_invalid_helo_hostname,
        reject_non_fqdn_helo_hostname

smtpd_sender_restrictions =
        permit_mynetworks,
        permit_sasl_authenticated,
        reject_non_fqdn_sender
#        reject_unknown_sender_domain #dla domen nie istniejących np na
serwerach swoich

smtpd_relay_restrictions =
        permit_mynetworks,
        permit_sasl_authenticated,
        defer_unauth_destination

mime_header_checks = pcre:/etc/postfix/mime_header_checks.pcre

# Even more Restrictions and MTA params
disable_vrfy_command = yes
strict_rfc821_envelopes = yes
smtpd_delay_reject = yes
smtpd_helo_required = yes
smtp_always_send_ehlo = yes
#smtpd_hard_error_limit = 1
smtpd_timeout = 30s
smtp_helo_timeout = 15s
smtp_rcpt_timeout = 15s
```

```
smtpd_recipient_limit = 40
minimal_backoff_time = 180s
maximal_backoff_time = 3h

relay_domains =
mailbox_command =

smtpd_sasl_local_domain = $myhostname
smtpd_sasl_auth_enable = yes
broken_sasl_auth_clients = yes

smtputf8_enable = no

# Reply Rejection Codes
invalid_hostname_reject_code = 550
non_fqdn_reject_code = 550
unknown_address_reject_code = 550
unknown_client_reject_code = 550
unknown_hostname_reject_code = 550
unverified_recipient_reject_code = 550
unverified_sender_reject_code = 550

# Handing off local delivery to Dovecot's LMTP, and telling it where to
store mail
virtual_transport = lmtp:unix:private/dovecot-lmtp

# Virtual domains, users, and aliases
virtual_mailbox_domains = mysql:/etc/postfix/mysql-virtual-mailbox-
domains.cf
virtual_mailbox_maps = mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf
virtual_alias_maps = mysql:/etc/postfix/mysql-virtual-alias-maps.cf,
        mysql:/etc/postfix/mysql-virtual-email2email.cf

maximal_queue_lifetime = 1d
bounce_queue_lifetime = 1d
```

Tworzymy plik /etc/postfix/mime_header_checks.pcre i uzupełniamy:

```
/^Content-(Disposition|Type).*name\s*\*?=\s*"?([^;]*(\.|=2E)(
        app|bat|chm|cmd|com|cpl|diagcab|dll|exe|fxp|gadget|grp|
        hlp|hpj|hta|htc|inf|ins|img|iso|isp|its|jar|jnlp|js|jse|
        ksh|lnk|mad|maf|mag|mam|maq|mar|mas|mat|mau|mav|maw|mcf|
        mda|mdw|mdz|msc|msh|msh1|msh2|mshxml|msh1xml|msh2xml|msi|
        msp|mst|msu|ops|osd|pcd|pif|plg|prf|prg|printerexport|
        ps1|ps1xml|ps2|ps2xml|psc1|psc2|psd1|psdm1|py|pyc|pyo|
        pyw|pyz|pyzw|reg|scf|scr|sct|shb|shs|theme|tmp|url|vb|
        vbe|vbp|vbs|vhd|vhdx|vsmacros|vsw|webpnp|website|ws|wsc|
        wsf|wsh|xbap|xll|xnk))(\?=)?"?\s*(;|$)/x
        REJECT Attachment of type $2 not accepted
```

Tworzymy plik /etc/postfix/mysql-virtual-mailbox-domains.cf i uzupełniamy:

```
user = postfix
password = tajnehaslo
hosts = 127.0.0.1
dbname = postfix
query = SELECT 1 FROM virtual_domains WHERE name='%s'
```

Tworzymy plik /etc/postfix/mysql-virtual-mailbox-maps.cf i uzupełniamy:

```
user = postfix
password = tajnehaslo
hosts = 127.0.0.1
dbname = postfix
query = SELECT 1 FROM virtual_users WHERE email='%s'
```

Tworzymy plik /etc/postfix/mysql-virtual-alias-maps.cf i uzupełniamy:

```
user = postfix
password = tajnehaslo
hosts = 127.0.0.1
dbname = postfix
query = SELECT destination FROM virtual_aliases WHERE source='%s'
```

Tworzymy plik /etc/postfix/mysql-virtual-email2email.cf i uzupełniamy:

```
user = postfix
password = tajnehaslo
hosts = 127.0.0.1
dbname = postfix
query = SELECT email FROM virtual_users WHERE email='%s'
```

Tworzymy plik /etc/postfix/mysql-virtual-access-ip.cf i uzupełniamy:

```
user = postfix
password = tajnehaslo
hosts = 127.0.0.1
dbname = postfix
query = SELECT CONCAT(access, IF(reason != '', CONCAT(' ', reason), '')) AS
address FROM virtual_black_white_list WHERE source='%s' AND type = 'IP'
```

Tworzymy plik /etc/postfix/mysql-virtual-access-email.cf i uzupełniamy:

```
user = postfix
password = tajnehaslo
hosts = 127.0.0.1
dbname = postfix
query = SELECT CONCAT(access, IF(reason != '', CONCAT(' ', reason), '')) AS
address FROM virtual_black_white_list WHERE source='%s' AND type = 'EMAIL'
```

Tworzymy plik /etc/postfix/mysql-virtual-sender-login-maps.cf i uzupełniamy:

```
user = postfix
password = tajnehaslo
hosts = 127.0.0.1
dbname = postfix
query = SELECT email FROM virtual_users WHERE email = '%s' UNION SELECT
destination FROM virtual_aliases WHERE source = '%s'
```

Modyfikujemy plik /etc/postfix/master.cf:

```
smtp      inet  n       -       n       -       -       smtpd
submission inet n       -       y       -       -       smtpd
  -o syslog_name=postfix/submission
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_sasl_type=dovecot
  -o smtpd_sasl_path=private/auth
  -o smtpd_reject_unlisted_recipient=no
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING#  -o
smtpd_reject_unlisted_recipient=no
smtps     inet  n       -       y       -       -       smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_sasl_type=dovecot
  -o smtpd_sasl_path=private/auth
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
pickup    unix  n       -       y       60      1       pickup
cleanup   unix  n       -       y       -       0       cleanup
qmgr      unix  n       -       n       300     1       qmgr
tlsmgr    unix  -       -       y       1000?   1       tlsmgr
rewrite   unix  -       -       y       -       -       trivial-rewrite
bounce    unix  -       -       y       -       0       bounce
defer     unix  -       -       y       -       0       bounce
trace     unix  -       -       y       -       0       bounce
verify    unix  -       -       y       -       1       verify
flush     unix  n       -       y       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
smtp      unix  -       -       y       -       -       smtp
relay     unix  -       -       y       -       -       smtp
showq     unix  n       -       y       -       -       showq
error     unix  -       -       y       -       -       error
retry     unix  -       -       y       -       -       error
discard   unix  -       -       y       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       y       -       -       lmtp
anvil     unix  -       -       y       -       1       anvil
scache    unix  -       -       y       -       1       scache
```

```
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail
($recipient)
ifmail    unix  -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix  -       n       n       -       -       pipe
  flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender
$recipient
scalemail-backend unix  -       n       n       -       2       pipe
  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store
${nexthop} ${user} ${extension}
mailman   unix  -       n       n       -       -       pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  ${nexthop} ${user}
```

Uprawnienia:

```
chmod -R o-rwx /etc/postfix
chmod 755 /etc/postfix
chmod 644 /etc/postfix/dynamicmaps.cf
chmod 644 /etc/postfix/main.cf
```

Aliasy. W pliku /etc/aliases edytujemy i ustawiamy wpis:

```
...
root: naszemail@domain.ltd
```

Aktualizujemy bazę aliasów:

```
newaliases
```

Restart Postfixa:

```
systemctl restart postfix
```

Dovecot

Jeśli mamy swoją konfigurację już na serwerze to robimy backup plików Dovecot:

```
cd /etc/dovecot
for f in ./dovecot* ; do cp $f $f.bak; done
cd conf.d
for f in ./* ; do cp $f $f.bak; done
/etc/init.d/dovecot stop
```

Linki symboliczne do logów (opcjonalne):

```
ln -s /var/log /etc/dovecot/logs
ln -s /var/mail/vhosts /etc/dovecot/vhosts
```

Edytujemy plik /etc/dovecot/dovecot.conf:

```
!include_try /usr/share/dovecot/protocols.d/*.protocol
protocols = imap pop3 lmtp

postmaster_address=postmaster at domain.ltd

dict {
  #quota = mysql:/etc/dovecot/dovecot-dict-sql.conf.ext
  #expire = sqlite:/etc/dovecot/dovecot-dict-sql.conf.ext
}

!include conf.d/*.conf
!include_try local.conf
```

Edytujemy plik /etc/dovecot/dovecot-sql.conf.ext:

```
driver = mysql
connect = host=127.0.0.1 dbname=postfix user=postfix password=tajnehaslo
default_pass_scheme = SHA512-CRYPT
password_query = SELECT email as user, password FROM virtual_users WHERE
email='%u';
user_query = SELECT concat('*:storage=', quota, 'M') AS quota_rule FROM
virtual_users WHERE email='%u';
iterate_query = SELECT email FROM virtual_users;
```

Edytujemy plik /etc/dovecot/conf.d/10-auth.conf:

```
disable_plaintext_auth = yes
auth_mechanisms = plain login

#!include auth-system.conf.ext
!include auth-sql.conf.ext
```

Edytujemy plik /etc/dovecot/conf.d/10-mail.conf:

```
mail_location = maildir:/var/mail/vhosts/%d/%n/
mail_home = /var/mail/vhosts/%d/%n/

namespace inbox {
  inbox = yes
}

mail_uid = vmail
mail_gid = vmail

mail_privileged_group = vmail
```

```
mail_plugins=quota

protocol !indexer-worker {

}
```

Edytujemy plik /etc/dovecot/conf.d/10-master.conf:

```
service imap-login {
  inet_listener imap {
    port = 0
  }
  inet_listener imaps {
    port = 993
    ssl = yes
  }
}

service pop3-login {
  inet_listener pop3 {
    port = 0
  }
  inet_listener pop3s {
    port = 995
    ssl = yes
  }
}

service submission-login {
  inet_listener submission {
    #port = 587
  }
}

service lmtp {
  unix_listener /var/spool/postfix/private/dovecot-lmtp {
    mode = 0600
    user = postfix
    group = postfix
  }
}

service imap {
  # Most of the memory goes to mmap()ing files. You may need to increase
this
  # limit if you have huge mailboxes.
  #vsz_limit = $default_vsz_limit

  # Max. number of IMAP processes (connections)
  #process_limit = 1024
}
```

```
service pop3 {
  # Max. number of POP3 processes (connections)
  #process_limit = 1024
}

service submission {
  # Max. number of SMTP Submission processes (connections)
  #process_limit = 1024
}

service auth {
  unix_listener /var/spool/postfix/private/auth {
    mode = 0660
    user = postfix
    group = postfix
  }

  unix_listener auth-userdb {
    mode = 0600
    user = vmail
  }

  user = dovecot
}

service auth-worker {
  user = vmail
}

service dict {
  # If dict proxy is used, mail processes should have access to its socket.
  # For example: mode=0660, group=vmail and global mail_access_groups=vmail
  unix_listener dict {
    #mode = 0600
    #user =
    #group =
  }
}

service quota-status {
  executable = quota-status -p postfix
  inet_listener {
    port = 12340
    # You can choose any port you want
  }
  client_limit = 1
}
```

Edytujemy plik /etc/dovecot/conf.d/10-ssl.conf:

```
ssl = required
```

```
ssl_cert = </etc/ssl/private/ssl.crt
ssl_key = </etc/ssl/private/ssl.key
ssl_client_ca_dir = /etc/ssl/certs
ssl_dh = </usr/share/dovecot/dh.pem
```

Edytujemy plik /etc/dovecot/conf.d/15-lda.conf:

```
postmaster_address = root@domain.ltd
hostname = domain.ltd
protocol lda {
  # Space separated list of plugins to load (default is global
mail_plugins).
  mail_plugins = $mail_plugins sieve
}
```

Edytujemy plik /etc/dovecot/conf.d/15-mailboxes.conf:

```
namespace inbox {
  mailbox Drafts {
    auto = subscribe
    special_use = \Drafts
  }
  mailbox Junk {
    auto = subscribe
    special_use = \Junk
  }
  mailbox Trash {
    auto = subscribe
    special_use = \Trash
  }
  mailbox Sent {
    auto = subscribe
    special_use = \Sent
  }
}
```

Edytujemy plik /etc/dovecot/conf.d/20-imap.conf:

```
protocol imap {
  # Space separated list of plugins to load (default is global
mail_plugins).
  mail_plugins = $mail_plugins imap_quota

  # Maximum number of IMAP connections allowed for a user from each IP
address.
  # NOTE: The username is compared case-sensitively.
  mail_max_userip_connections = 20
}
```

Edytujemy plik /etc/dovecot/conf.d/20-lmtp.conf:

```
protocol lmtp {
  # Space separated list of plugins to load (default is global
mail_plugins).
  mail_plugins = sieve
}
```

Edytujemy plik /etc/dovecot/conf.d/20-managesieve.conf:

```
protocols = $protocols sieve

service managesieve-login {
  inet_listener sieve {
    port = 4190
  }
}

service managesieve {
  #process_limit = 1024
}

protocol sieve {
  managesieve_max_line_length = 65536
  #managesieve_implementation_string = Dovecot Pigeonhole
  managesieve_implementation_string = dovecot
  #log_path = /var/log/dovecot-sieve-errors.log
  #info_log_path = /var/log/dovecot-sieve.log
}
```

Edytujemy plik /etc/dovecot/conf.d/20-pop3.conf:

```
protocol pop3 {
  mail_plugins = $mail_plugins
  mail_max_userip_connections = 20
}
```

Edytujemy plik /etc/dovecot/conf.d/90-quota.conf:

```
plugin {
  quota = maildir:User quota
  quota_exceeded_message = User %u has exhausted allowed storage space.

  quota_status_success=DUNNO
  quota_status_nouser=DUNNO
  quota_status_overquota="552 5.2.2 Mailbox is full"
}
```

Edytujemy plik /etc/dovecot/conf.d/90-sieve-extprograms.conf:

```
service managesieve-login {
  inet_listener sieve {
```

```
    port = 4190
  }
}

service managesieve {
}

protocol sieve {
    managesieve_max_line_length = 65536
    managesieve_implementation_string = dovecot
    #log_path = /var/log/dovecot-sieve-errors.log
    #info_log_path = /var/log/dovecot-sieve.log
}
```

Edytujemy plik /etc/dovecot/conf.d/90-sieve.conf:

```
plugin {
  sieve_extensions = +vacation-seconds
  sieve_vacation_min_period = 5m
  sieve_vacation_default_period = 10m
  sieve_vacation_max_period = 15m

  sieve = /var/mail/vhosts/%d/%n/dovecot.sieve
  sieve_default = /var/lib/dovecot/sieve/default.sieve
  sieve_global = /var/lib/dovecot/sieve/global/
  sieve_dir = /var/mail/vhosts/%d/%n/sieve
}
```

Edytujemy plik /etc/dovecot/conf.d/auth-sql.conf.ext:

```
passdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
}

userdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
}
```

Tworzymy katalog /var/lib/dovecot/sieve:

```
mkdir /var/lib/dovecot/sieve
```

Tworzymy i edytujemy plik /var/lib/dovecot/sieve/default.sieve:

```
require ["fileinto"];
# rule:[SPAM]
if header :contains "X-Spam-Flag" "YES" {
fileinto "Junk";
```

```
}
```

Uprawnienia:

```
chown -R root:dovecot /etc/dovecot
chmod -R o-rwx /etc/dovecot
```

Restart Dovecot oraz wydajemy polecenie obliczania quot:

```
systemctl restart dovecot
doveadm quota recalc -u vmail
```

DNS

Aby domena działała prawidłowo to rekordy domeny powinny być ustawione:

- rekord MX główny domeny powinien wskazywać na adres serwera poczty, np: domain.ltd MX 1 domain.ltd
- rekord A na który wskazuje rekord MX powinien mieć wpisany adres IP naszego serwera poczty np: domain.ltd A 1.2.3.4
- zaleca się, aby też ustawić rekord SPF, w którym zapisze, z jakich adresów IP będzie można wysyłać pocztę w naszej domenie np: domain.ltd TXT 'v=spf1 ip4:1.2.3.4 -all'

Webmail

Instalujemy Roundcube:

```
aptitude install roundcube roundcube-mysql roundcube-plugins roundcube-
plugins-extra
```

Dodajemy do konfiguracji szyfrowanie:

```
ln -s /etc/apache2/mods-available/socache_shmcb.load /etc/apache2/mods-
enabled/socache_shmcb.load
ln -s /etc/apache2/mods-available/ssl.load /etc/apache2/mods-
enabled/ssl.load
ln -s /etc/apache2/mods-available/ssl.conf /etc/apache2/mods-
enabled/ssl.conf
ln -s /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-
enabled/000-default-ssl.conf
```

Edytujemy plik /etc/apache2/sites-enabled/000-default-ssl.conf i ustawiamy:

```
SSLCertificateFile /etc/ssl/private/ssl.crt
SSLCertificateKeyFile /etc/ssl/private/ssl.key
```

Podczas instalacji zostaniemy zapytani o hasło do bazy Roundcube, która zostanie utworzona - wybieramy Yes. Poprosi nas o wpisanie hasła - pozostawiamy puste - zostanie automatycznie

wygenerowane do pliku konfiguracji Roundcube.

Edytujemy plik /etc/apache2/conf-enabled/roundcube.conf i na samym początku pliku wpisujemy/odkomentujemy wpis:

```
Alias /roundcube /var/lib/roundcube
```

Resteart Apache2:

```
systemctl restart apache2
```

Edytujemy plik /var/lib/roundcube/config/config.inc.php - odszukujemy i ustawiamy:

```
...
$config['default_host'] = 'ssl://domain.ltd';
$config['imap_auth_type'] = "LOGIN";
$config['imap_conn_options'] = null;
...
$config['smtp_server'] = 'domain.ltd';
$config['smtp_port'] = 25;
$config['smtp_user'] = '%u';
$config['smtp_pass'] = '%p';
$config['smtp_auth_type'] = 'LOGIN';
...
$config['plugins'] = array('managesieve');
...
```

Edytujemy plik /var/lib/roundcube/plugins/managesieve/config.inc.php:

```
<?php
$config=array();
$config['managesieve_port'] = 4190;
$config['managesieve_host'] = '127.0.0.1';
$config['managesieve_auth_type'] = null;
$config['managesieve_auth_cid'] = null;
$config['managesieve_auth_pw'] = null;
$config['managesieve_usetls'] = false;
$config['managesieve_conn_options'] = null;
$config['managesieve_default'] = '/var/lib/dovecot/sieve/global';
$config['managesieve_script_name'] = 'managesieve';
$config['managesieve_mbox_encoding'] = 'UTF-8';
$config['managesieve_replace_delimiter'] = '';
$config['managesieve_disabled_extensions'] = array();
$config['managesieve_debug'] = false;
$config['managesieve_kolab_master'] = false;
$config['managesieve_filename_extension'] = '.sieve';
$config['managesieve_filename_exceptions'] = array();
$config['managesieve_domains'] = array();
$config['managesieve_default_headers'] = array('Subject', 'From', 'To');
$config['managesieve_vacation'] = 1;
$config['managesieve_forward'] = 1;
```

```
$config['managesieve_vacation_interval'] = 0;
$config['managesieve_vacation_addresses_init'] = false;
$config['managesieve_vacation_from_init'] = false;
$config['managesieve_notify_methods'] = array('mailto');
$config['managesieve_raw_editor'] = true;
$config['managesieve_disabled_actions'] = array();
$config['managesieve_allowed_hosts'] = null;
```

Aby otworzyć webmaila otwieramy stronę: https://domain.ltd/roundcube/

Auto konfiguracja klienta poczty

MS Outlook dosyć dobrze radzi sobie z rozpoznaniem serwerów i konfiguracji pocztowej więc moje próby związane z auto-konfiguracją Outlooka więcej złego robiły niż dobrego. Thunderbird gorzej sobie radzi, ale możemy jemu podpowiedzieć jak ma to robić wystawiając na serwerze webowym plik konfiguracji.

Tworzymy katalog:

```
mkdir -p /var/www/html/.well-known/autoconfig/mail
```

Zapisujemy do pliku /var/www/html/.well-known/autoconfig/mail/config-v1.1.xml zawartość:

```
<?xml version="1.0" encoding="UTF-8"?>

<clientConfig version="1.1">
  <emailProvider id="domain.ltd">
    <domain>domain.ltd</domain>
    <displayName>domain.ltd</displayName>
    <displayShortName>domain.ltd</displayShortName>
    <incomingServer type="imap">
      <hostname>domain.ltd</hostname>
      <port>993</port>
      <socketType>SSL</socketType>
      <authentication>password-cleartext</authentication>
      <username>%EMAILADDRESS%</username>
    </incomingServer>
    <incomingServer type="pop3">
      <hostname>domain.ltd</hostname>
      <port>995</port>
      <socketType>SSL</socketType>
      <authentication>password-cleartext</authentication>
      <username>%EMAILADDRESS%</username>
    </incomingServer>
    <outgoingServer type="smtp">
      <hostname>domain.ltd</hostname>
      <port>465</port>
      <socketType>SSL</socketType>
      <authentication>password-cleartext</authentication>
      <username>%EMAILADDRESS%</username>
```

```
    </outgoingServer>
    <outgoingServer type="smtp">
      <hostname>domain.ltd</hostname>
      <port>587</port>
      <socketType>STARTTLS</socketType>
      <authentication>password-cleartext</authentication>
      <username>%EMAILADDRESS%</username>
    </outgoingServer>
  </emailProvider>
</clientConfig>
```

Klient poczty

Porty:

- SMTP: 465 (SSL/TLS) 587 (STARTTLS)
- POP3: 995 (SSL/TLS)
- IMAP: 993 (SSL/TLS)

Fail2Ban

Instalujemy:

```
apt install fail2ban
```

W pliku /etc/fail2ban/jail.conf ustawiamy:

```
...
ignoreip = 127.0.0.1/8 ::1
...
bantime  = 60m
...
findtime  = 60m
...
[roundcube-auth]
port     = http,https
logpath  = %(roundcube_errors_log)s
enabled = true
...
[postfix-sasl]
enabled = true
filter   = postfix[mode=auth]
port     = smtp,465,submission,imap,imaps,pop3,pop3s
# You might consider monitoring /var/log/mail.warn instead if you are
# running postfix since it would provide the same log lines at the
# "warn" level but overall at the smaller filesize.
logpath  = %(postfix_log)s
backend  = %(postfix_backend)s
```

```
...
```

Restart:

```
/etc/init.d/fail2ban restart
```

Status fail2bana sprawdzamy poleceniem:

```
root@mars:/var/log# fail2ban-client status
Status
|- Number of jail:      3
`- Jail list:   postfix-sasl, roundcube-auth, sshd
root@mars:/var/log# fail2ban-client status postfix-sasl
Status for the jail: postfix-sasl
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/mail.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

Munin

Monitoring zasobów serwera.

Instalacja:

```
apt install munin munin-node munin-plugins-extra
```

Konfigurujemy plik /etc/munin/apache24.conf:

```
ScriptAlias /munin-cgi/munin-cgi-graph /usr/lib/munin/cgi/munin-cgi-graph
Alias /munin/static/ /var/cache/munin/www/static/

<Directory /var/cache/munin/www>
    #Require local
    Require ip nasz_adres_ip
    Options FollowSymLinks SymLinksIfOwnerMatch
    Options None
</Directory>

<Directory /usr/lib/munin/cgi>
    #Require local
    Require ip nasz_adres_ip
    Options FollowSymLinks SymLinksIfOwnerMatch
    <IfModule mod_fcgid.c>
        SetHandler fcgid-script
```

```
    </IfModule>
    <IfModule !mod_fcgid.c>
        SetHandler cgi-script
    </IfModule>
</Directory>

Alias /munin /var/cache/munin/www
```

Reload konfiguracji Apache:

```
systemctl apache2 reload
```

Munin będzie dostępny pod: http://domain.ltd/munin

Przydatne narzędzia

- postqueue

```
# postqueue -p
-Queue ID-  --Size-- ----Arrival Time---- -Sender/Recipient-------
56008207DE   195074 Mon Mar 22 09:28:19  user@domain.ltd
                  (connect to falsedomain.ltd[1.2.3.4]:25: Connection
refused)
                                         user44@falsedomain.ltd

-- 190 Kbytes in 1 Request.
```

- postsuper

```
# postsuper -d 56008207DE
postsuper: 56008207DE: removed
postsuper: Deleted: 1 message
```

- postmap

```
# postmap -q 'name="fil.cmd"' regexp:/etc/postfix/mime_header_checks
REJECT
# postmap -q 'Content-Type: name="test.img"; charset=us-ascii'
pcre:/root/mime.pcre
REJECT Attachment of type test.img not accepted
```

- rblcheck

```
rblcheck -s dnsbl.sorbs.net adresiplubdomena
```

- przenoszenie skrzynek pocztowych via IMAP: https://github.com/imapsync/imapsync
- sprawdzanie czy nasza domena jest na czarnych listach: https://mxtoolbox.com
- tester naszego serwera: https://www.mail-tester.com
- sprawdzanie DNSów naszej domeny: https://intodns.com
- sprawdzanie czy nasz adres IP lub domena jest na czarnych listach: https://www.spamhaus.org/lookup/

- Dodanie naszej domeny do zaufanych w Google: https://postmaster.google.com/
- Dodanie naszej domeny do zaufanych w Microsoft: https://sendersupport.olc.protection.outlook.com/pm/
- Sprawdzenie domeny oraz maili: https://bezpiecznapoczta.cert.pl